#23 Sub

See (N.C)

2-23-98

Consider as part of
formal amendment
T. Tarcza 3/13/98

Do Not
Enter
Int

SUBSTITUTE SPECIFICATION

Software for restricting other software to be used by the rightful user only

Field of the invention

The present invention relates to protection of commercial software supplied through a communication link or the like, and particularly, to protection of such software against unauthorised use.

Background of the invention

Conventionally, software protection methods for protecting commercial software products such as programs, multimedia software, supplied through a communication link, such as a telephone line, require a user computer to have a piece of hardware which comprises, for instance, decryption keys and system be installed therein for to be authenticated by a software program running on the computer. Hardware, rather than software, are being used because software duplication facilities are commonly found in personal computers. However, this is extremely cumbersome and places a large burden on users and vendors alike.

It is therefore an object of the present invention to provide a piece of software to replace the above-mentioned piece of hardware and its rightful user is being discouraged from copying it to someone else.

Summary of the invention

According to a first embodiment of the present invention, there is provided a central program comprising 1) a program for providing an Encrypted Identity (hereinbelow referred to as EI program), 2) a program for authorising use of a software product (hereinbelow referred to as ES program), 3) a program for authenticating user computer (hereinbelow referred to as AC program).

The central program is for managing the use of the individual programs therein so that the ES program can be protected from being copied individually. The EI program is for providing an encrypted identity of a user for accessing a network central computer to obtain services or software products or alike inwhich a secure operation on a user account for payment therefor involved. The AC program is for authenticating the computer on which it runs by determining the hardware and software configuration as well as hardware charateristics of the computer by software means and comparing the result with that required. The ES program is for using the authentication result of the AC program and the presence of the EI program as preconditions for authorising those software products obtained to be used on a computer.

It should be noted that in the central program, as far as protection of the software products from being unlawfully copied by the rightful user to someone else is concerned, the ES program is the one which needs protection and according to the present invention, the ES program is protected from being unauthorised copied by its rightful user to someone else lies on the fact that a rightful user would not copy a program, i.e., the EI program, which can provide the rightful user's encrypted identity for using the rightful user's account in obtaining, for eg., network services or software products, to someone else. As seen from the use of automatic teller machine(ATM) magnetic cards, which although can readily be forged, has been proved to be remarkably secure.

According to a second embodiment of the present invention, the central program comprising the EI program only, and the ES program authorises the software product(s) to be used only when the EI program is present on the same computer and which is being determined by receiving an encrypted identity of the EI program from the same.

According to a third embodiment, the EI and ES programs are basically equivalent such that copying the ES program by its rightful user to someone else is equivalent to copying the EI program to someone else, thereby preventing the ES program from unauthorised copied or use.

Brief description of drawings

FIG.1 is a block diagram of the central program.

FIG.2 is a diagrammatic view of a program inwhich a part B thereof being encrypted, in RAM space.

Detailed description of the preferred embodiments

The present invention is directed to protecting software product(s) supplied through a communication link, and for the sake of simplicity, the following description is directed to protection of such software product(s) stored in a user's IBM PC computer, against unauthorised copying or use. And, the present invention will be described under the following headings:

1) The Central Program.

2) The Program for providing an Encrypted Identity (EI program).

3) The Program for authorising use of a software product (ES program).

4) The Program for authenticating user computer (AC program).

5) Other Embodiments.

1) The Central Program.

According to the first embodiment, there is provided a central program which being an executable program and can be caused to be executed a) by user by entering its filename in DOS environment, b) by a running program. FIG.1 is a block diagram of the central program.

a) If a user desires to access a network central computer through a communication link, the user has to cause the central program to be executed.

Then the central program will cause the EI program, of which details will be described herein below, to be executed for providing an encrypted identity of the user, to the central computer. The central computer will permit the access request from the user if the encrypted identity is correct, for which details will be described in item 2 herein below.

b) When a running program desires to cause the ES program to be executed, to authorise it to continue to run, it will first prepare an input parameter for indicating to the central program such a request and store the input parameter in a predetermined location in RAM, then through the use of a PC DOS service call for that purpose, cause the central program to be executed. The central program will first access the input parameter in the predetermined location and from it the central program can determine that a running program is requesting for an authorisation command from the ES program, and will then cause the ES program to be executed.

For the case the central program is being caused by user to be executed, there will be no valid or no input parameter and the central program can thus know this fact.

2) The Program for providing an Encrypted Identity (EI program).

This program borrows the technique used in IC credit card for identity authentication inwhich an encrypted identity is generated.

When starts, the EI program sends an access request to the central computer which in return will send back a random number. The EI program will then encrypt the random number with a predetermined algorithm A1 and send the result to the central computer which will permit access if the result is identical with another result it obtained by performing the same encryption algorithm on that random number.

It should be noted that for each user, there is a corresponding respective encryption algorithm A1 for the identification thereof and also that the central computer may use the encryption result from the EI program, if it being correct, as a user authorisation for payment to be made, from a user account for obtaining network services or software products or the like.

3) The Program for authorising use of a software product (ES program).

According to the present invention, there are 2 approaches for authorising use of a software product :

i) by sending encrypted commands to a running software program for authorising continuous use of the same on a computer, by the technique as mentioned above in item 2 for identity authentication. Specifically, the running software program includes in the input parameter, as mentioned above in item 1b, a random number it generated, then causes the central program to be executed. The ES program, which being caused to be executed by the central program, as mentioned above in item 1b, sends the result it obtained by performing a predetermined encryption algorithm A2 on that random number, to the running software program which will compare the result with another result it obtained by performing the same encryption algorithm A2 on that random number.

It should be noted that for each user, each of the software products for use on his/her computer(s) use a same respective encryption algorithm A2 and the encryption algorithm A2 being included into each such software product by the central computer at the time when the central computer is to supply the same to the user computer.

ii) by decrypting an encrypted part of a software product or an encrypted software product.

It should be noted that if the software product is a program, then it will be sufficient to have a part thereof to be encrypted, for preventing unauthorised copying and use, however, if the software product is an audio/visual multimedia data file, it should be more desirable to have the whole software product be encrypted.

The decryption of a part of or an entire software product takes place on a temporary copy of which in RAM. Given by example only, FIG. 2 is a diagrammatic view of a program in RAM space, with a part B thereof being encrypted. As seen, the ES program decrypts part B and stores the result which size should be not equivalent to that of the encrypted copy, in 'part B decrypted'.

The ES program then overwrites at the first location of 'part B encrypted' an instruction 'JUMP TO part B decrypted' and at the end of 'part B decrypted' appends an instruction 'JUMP TO part C'. In this way, the encrypted part of the software will not be executed and the decrypted part will be executed instead.

In the case of audio/visual multimedia software, the software will be decrypted a small part by a small part and each small part is decrypted at the time it is about to be utilized by a audio/visual program for causing audio/visual effect. In other words, that audio/visual program has to cause the ES program to be executed in the manner as described above in item 1b, everytime it wants a decryption of a small part. Desirably, a newly decrypted small part will overwrite a previously decrypted one so that a whole copy of the decrypted software will not exist in RAM.

4) The Program for authenticating user computer (AC program).

One object of this program is to prevent the central program from being used , if it being a copy made by someone other than the rightful user and of this the rightful user being unaware, so that a rightful user need not guard his computer containing the central program from reach of someone else.

When the central program is being installed in a harddisk of a user computer and executed, it will check an encrypted status information stored in itself and from which it knows this is the first time it being executed and will cause an initialization process to take place. In the initialization process, the central program sends to the central computer, as mentioned herein above in item 2, an unencrypted identity of the user, then the AC program requests for an encrypted command from the central computer which will provide such an encrypted command, in the manner as described hereinabove in item 3i, if the user has a valid account or the account is not closed.

After authenticating the command, the AC program determines the hardware and software configuration of the user computer, which includes, for eg., running speed determination which is a function of CPU frequency, cache memory size etc; number and identities of peripherals such as mouse, printer, joystick, harddisk and floppy disk drive etc; characteristics of hardware such as number of heads, cylinders, sectors of harddisk and locations of bad sectors therein; version number of operation system software and physical position of a particular software product including the central program in the harddisk; by skills well known to those in the art. For instance, the running speed can be determined by causing the computer to execute a test program and initializing a hardware counter to measure the time the computer has taken to finish executing the program. For another instance, the version number of the operation system may be determined by using a particular DOS service call.

The result of the determination and a status information indicative of the central program being initialized is being stored by the AC program in a predetermined part of the central program in the harddisk, in the form of encrypted data. Thereafter, everytime when the central program is executed, it will first check the status information, and after determining that it is being initialized, it will perform a job as requested, as mentioned in item 1 herein above, and in addition thereto, it will also automatically cause the AC program to be executed which will determine at least a part of the above-mentioned hardware and software configuration as well as

hardware characteristics of the computer, at a time, and the AC program will encrypt an indication information in another predetermined part of the central program for causing the ES program not to operate, if any part of the configuration/characteristics determined is not identical to the corresponding part of that it encrypted and stored previously.

In addition thereto, the AC program will also reset the encrypted status information so that another initialization process will automatically take place when the user causes the central program to be executed, and for the authorisation of which another encrypted command from the central computer will be required.

This also prevents a user from deliberately adapting the central program to computer of other user(s), after closing his account.

In addition, the encrypted command from the central computer may alternatively be supplied to the user via, eg., a telephone line, and then entered into the user computer by the user. Specifically, to request for an encrypted command, the AC program generates a random number and conveys the random number to the user who in turn supplies it to the central computer by means of telephone dual tone signals, generated by entering the random number on a telephone keypad, through the telephone line, and after encrypting the random number, the central computer sends the result to the user via the same telephone line by means of a voice synthesizer.

5) Other Embodiments

According to the second embodiment, the ES program is separated from the central program which comprises the EI program only. The ES program is bound to the EI program by requiring the ES program to operate only when the EI program is present on the same computer. Specifically, the ES program when running, can cause the EI program to be executed for generating an encrypted identity for the ES program to authenticate. The EI program knows that this is a request for encrypted identity from the ES program, not a request from user for encrypted identity for accessing the

central computer, by the technique of input parameter as mentioned above in item 1b.

Further, the EI program before sending the encrypted identity to the ES program, may first check the data integrity of itself by, for instance, checksum method. Alternatively, it may also be that the ES program performs the checking. And, if the checking result is that some data in the EI program being altered, then in the former case, the ES will be caused to be not operable by the EI program by not sending it an encrypted identity, and in the latter case, the ES program will be caused to be not operable by itself.

According to the third embodiment, the encryption algorithms A1 and A2 that the EI and ES programs use respectively for providing an encrypted identity to the central computer and for generating encrypted commands to authorise use of a software product respectively, is a same algorithm.

Thus, it would be equivalent for a rightful user to copy his EI program to someone else if he copies his ES program to someone else. In this case, a slight modification on the ES program can make it equivalent to the EI program and which involves adding a simple interface program for receiving a random number from the central computer, feeding the random number into the ES program, receiving the encryption result from the ES program and supplying the encryption result to the central computer, and such functions are commonly found in any network interface software.

In addition, according to another embodiment of the present invention, the software products and ES program each includes an identity of its rightful user, so as to facilitate legal action against piracy. Further, the ES program, when executed, will access each of the software products, by using a particular DOS service call for loading a software product stored in the computer onwhich it runs, from harddisk to RAM, for checking such an identity therein, if any software product is found to have an identity not identical to that of the ES program, the ES program will inhibit use of all software products under its control, including itself, on the computer.

Such identities may be stored in a predetermined location of the software products, and is protected from being altered by having an encrypted one stored in another location in each software product, and each of those another locations is different in different software products so that it would not be discovered and altered. And, each such software product, when executed, will automatically check the unencrypted identity stored therein against the decryption result of the encrypted one, if they are not consistent, the software product will fail to operate. The identity or encrypted identity of the rightful user being included into each of the software products by the central computer at the time when the central computer is to supply the same to the user computer. Further, to prevent the ES program from mistakenly regarding a software product which stored in the computer and which being not supplied from the central computer, as a software product under its control, the central computer may further include information in another predetermined location of each software product for indicating this fact, that is, the software product being supplied from the central computer, to the ES program and each software product will not operate if when being executed, it finds that information therein being altered.